29. (New) The system of claim 28, wherein at least one security association (SA) is stored in said memory.

30. (New) The system of claim 29, further including a network driver to parse said encrypted packet, to match said encrypted packet with one of said at least one SA, and adapted to instruct a network interface to transfer said encrypted packet and said one SA across a bus to a controller.

31. (New) The system of claim 28, wherein said computer asserts an additional interrupt after completion of said decryption operation.

REMARKS

Claims 1-27 are pending. Claims 11 and 23-27 have been amended. Claims 28-31 have been added. Applicant respectfully requests examination and an action on the merits.

The Specification has been amended to properly reference various trademarks included therein. Applicants respectfully assert that the use of these trademarks is proper as they clearly identify the specific products to which they refer, and, as amended, are set forth in capital letters in the text of the Specification. MPEP § 608.01(v).

Claims 11 and 23-27 have been amended to correct typographical errors contained in the preambles thereof. Claim 11 initially described an "encrypted network system," and has been amended to describe a "computing system." Similarly, claims 23, 24, and 26 each initially described a "system," and claims 25 and 27 each initially described a "method." Each of these claims have been amended to describe a "device."

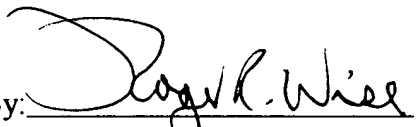
New claims 28-31 have been added to describe an embodiment of the invention. No new

matter has been added. New independent claim 28 describes a system including a computer and memory, in which the computer asserts an interrupt prior to a complete transfer of a decrypted packet to the memory. New dependent claims 29-31 describe various further embodiments of the system described in claim 28. Support for these additional claims may be found in the Specification at page 4, line 17 through page 5, line 6.

Respectfully submitted,

PILLSBURY WINTHROP LLP

Date: April 18, 2002

By: 

Roger R. Wise
Registration No. 31,204
Attorney For Applicant(s)

725 South Figueroa Street, Suite 2800
Los Angeles, CA 90017-5406
Telephone: (213) 488-7100
Facsimile: (213) 629-1033

APPENDIX

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE SPECIFICATION:

The specification is amended as follows:

At page 2, fourth paragraph:

From a performance perspective (both CPU utilization and throughput), Inline Receive is generally considered a better solution than Secondary Use. However, Inline Receive is more expensive to implement because the keys and matching information for cryptography operations must be stored on the network interface in an SA cache. Due to such limitations, the INTEL [Intel] PRO/100 S Server Adapter [Adapters], for example, supports [support] only a limited number of connections that can use Inline Receive. Other connections use the Secondary Use model to offload secure traffic, though Secondary Use adds latency to packets at several steps. The primary source of the increased latency for Secondary Use is the delay related to the final interrupt of the Secondary Use operation.

At page 8, third paragraph:

Decryption engines process data at a rate of approximately 600 Megabits per second ("Mbit/sec"). The latency from the device Interrupt Request line ("IRQ") to interrupt processing is based on measurements on INTEL PENTIUM [Intel Pentium] III Processor and INTEL PENTIUM [Pentium] 4 Processor systems using a [running] MICROSOFT WINDOWS [Microsoft Windows] 2000 Operating System. Notably, the value of this latency does not change significantly with processor speed.

IN THE CLAIMS:

The claims are amended as follows:

11. (Amended) The computing [encrypted network] system of claim 10, wherein said network driver parses said encrypted packet, matches said encrypted packet with one of said at least one SA and instructs said controller to transfer said encrypted packet and said one SA across said bus to said controller.

23. (Amended) The device [system] of claim 22, wherein prior to the instructions to convert said encrypted packet, said system further includes instructions to:

issue a decryption command to a controller; and

determine a time for said assertion of said interrupt in response to said decryption command.

24. (Amended) The device [system] of claim 22, wherein said instructions to convert said encrypted packet to said decrypted packet further includes instructions to:

parse said encrypted packet;

match said encrypted packet with a corresponding security association (SA) stored in said host memory; and

transfer said encrypted packet and said corresponding SA to a controller.

25. (Amended) The device [method] of claim 22, wherein said instructions to convert said encrypted packet to said decrypted packet further includes instructions to authenticate said decrypted packet.

26. (Amended) The device [system] of claim 22, further including instructions to assert an additional interrupt upon completion of said transfer of said decrypted packet to said host memory

27. (Amended) The device [method] of claim 22, further including instructions to indicate said decrypted packet to a protocol stack after the instruction to assert said interrupt.

28. (New) A system, comprising:

a computer to receive an encrypted packet and to perform a decryption operation that converts said encrypted packet into a decrypted packet; and

a memory included in said computer, said computer asserting an interrupt prior to a complete transfer of said decrypted packet to said memory.

29. (New) The system of claim 28, wherein at least one security association (SA) is stored in said memory.

30. (New) The system of claim 29, further including a network driver to parse said encrypted packet, to match said encrypted packet with one of said at least one SA, and adapted to instruct a network interface to transfer said encrypted packet and said one SA across a bus to a controller.

31. (New) The system of claim 28, wherein said computer asserts an additional interrupt after completion of said decryption operation.